We claim:

1. An integrated circuit for the authentication of a consumable storage device by an apparatus, the integrated circuit comprising a memory space which contains encrypted data defined by a message authentication code (MAC) applied to data relating to a consumable stored by the device and by at least one secret key (K) shared by the apparatus for decryption of the data, the MAC being a construction of a cryptographic function.

2. An integrated circuit as claimed in claim 1, in which the cryptographic function is a hash function such that the MAC is an algorithm known as HMAC.

3. An integrated circuit as claimed in claim 2 in which the hash function is one of an MD5 function and a SHA-1 function.

4. An integrated circuit as claimed in claim 2, in which the hash function is an SHA-1 function.

5. An integrated circuit as claimed in claim 4, which is configured to define a number of temporary registers and rotating counters and to calculate an output word on an iterative basis by calculating and allocating words to respective registers during processing of the SHA-1 function.

6. An integrated circuit as claimed in claim 1, in which the memory space of the integrated circuit includes two secret keys, K_1 and K_2, the integrated circuit being configured to that the key K_1 is used to decrypt an encrypted random number generated by the apparatus and the key K_2 is used to decrypt encrypted data stored in the memory space.

7. A method of encrypting data relating to a consumable of a consumable storage device for an apparatus and stored by an integrated circuit, the method including the steps of:

applying a message authentication code (MAC) to the data using at least one secret key shared by the apparatus to decrypt the data, the MAC being a construction of a cryptographic function.